Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) Method for digitally signing an electronic form in a secure manner by means of a mobile station, said method comprising the steps of:

computing a first hash code for the material to be signed, the material to be signed including the form, an identifier of the form, shared information, and/or essential information;

transferring the material to be signed and the first hash code ~~, which comprises the form, its identifier, shared information, and/or essential information added to it,~~ to the mobile station~~, characterised in that~~

~~a first hash code (H1) is computed from the material to be signed;~~

digitally signing, using the mobile station, the material and first hash code transferred to the mobile station ~~is signed digitally by means of the mobile station;~~ and

verifying the authenticity of the signed and transferred material ~~is verified~~ by comparing the signed hash code with the first hash code computed from the material before signature.

2. (currently amended) Method as defined in claim 1, ~~characterised in that~~ wherein the first hash code is added to the material[[,]] to be transferred to the mobile station.

3. (previously presented) Method as defined in claim 1, wherein the material to be signed is generated from an identifier of the form and essential information associated with the form.

4. (currently amended) Method as defined in claim 3, ~~characterised in that~~ wherein said step of computing comprises computing the first hash code from the material to be signed, ~~a first hash code is computed, preferably~~ before the material is transferred into the mobile station.

5. (currently amended) Method as defined in claim 1, wherein:

the material is transferred to the mobile station for signature ~~is transferred to~~ from a second party; and

the signed material is transferred to the second party, whereupon the second party ~~verifies~~ performs said step of verifying the authenticity of the signature.

6. (currently amended) Method as defined in claim [[1]] 5, wherein:

the material is encrypted before being transferred between the mobile station and the second party; and

the encrypted material is decrypted before any treatment of the material, such as signature and verification of authenticity.

7. (previously presented) Method as defined in claim 1, wherein the form is generated using a pre-agreed form template provided with an identifier, the essential information being filled in in the form template before it is transferred to the mobile station.

8. (previously presented) Method as defined in claim 1, wherein the hash code is generated using a hash function.

9. (previously presented) Method as defined in claim 1, wherein the signature and/or encryption of the message is implemented using a public and private key method.

10. (previously presented) Method as defined in claim 1, wherein the material and/or part of it is presented in the mobile station before the material is signed.

11. (previously presented) Method as defined in claim 1, wherein the mobile station is started in signature mode before the transfer of the material into the mobile station.

12. (previously presented) Method as defined in claim 1, wherein:

the material is stamped with a time stamp; and

the transaction of signature of the material is filed after the signature has been authenticated.

13. (currently amended) System for digitally signing an electronic form in a secure manner by ~~means of~~ a mobile station (MS), said system comprising:

a payment machine ~~(2)~~;

means ~~(3)~~ connected to the payment machine for the generation of the material to be signed, said material comprising a form, its identifier, shared data, and/or essential information added to it, and

means ~~(4)~~ connected to the payment machine for the transfer of the material into the mobile station ~~(MS)~~, ~~characterised in that~~ wherein

the payment machine comprises means ~~(5)~~ for computing a first hash code ~~(H1)~~ from the material to be signed and means for transfer of the first hash code into the mobile station;

the mobile station comprises signing means ~~(6)~~ for the signing of the material transferred into it; and

the payment machine comprises means ~~(7)~~ for verifying the authenticity of the signed and transferred material by comparing [[s]] the signed hash code ~~($H1_{ss}$)~~ with the first hash code ~~(H1)~~ computed from the material before signature.

14. (previously presented) System as defined in claim 13, wherein the system comprises:

a server connected to the payment machine and the mobile station and controlled by a third party; and

the mobile station comprises means for encrypting the signed material.

15. (previously presented) System as defined in claim 13, wherein the server comprises means for the verification of authenticity of the digital signature.

16. (currently amended) System as defined in claim 13, wherein the mobile station comprises means for presenting the material and/or part of ~~it~~ the material in the mobile station before the signing of the material.

17. (previously presented) System as defined in claim 13, wherein the server comprises:

means for stamping the material with a time stamp; and

means for filing the transaction of signing of the material after the signature has been authenticated.